

WHAT IS CLAIMED IS:

5

1. In an authentication system for authenticating users who are parties to a transaction, an authentication method comprising the steps of:

- 10 (a) supplying a first user with a matching key for a prospective transaction;  
(b) receiving at a second user the matching key supplied to the first user; and  
15 (c) matching the key supplied from the first user to the second user against the key supplied to the first user, after the second user has received the key from the first user.

20

2. The authentication method as claimed in claim 1, wherein the authentication system authenticates the identity of the users prior to the  
25 step of supplying the first user with the matching key.

30

3. The authentication method as claimed in claim 1, wherein the authentication system determines whether the proposed transaction is within a previously determined monetary limit.

35

2025 RELEASE UNDER E.O. 14176

4. The authentication method as claimed in  
claim 1, wherein the authentication system  
determines whether the proposed transaction  
5 satisfies previously determined conditions.

10 5. The authentication method as claimed in  
claim 1, wherein the step of supplying matching keys  
supplies different keys to both users.

15 6. The authentication method as claimed in  
claim 1, further comprising the steps of:

(d) supplying a matching key to the second  
20 user in a prospective transaction; and

(e) receiving at the first user the  
matching key supplied to the second user; and

(f) matching the key supplied from the  
second user to the first user with the key supplied  
25 from the first user to the second user.

30 7. The authentication method as claimed in  
claim 1, further comprising the step of payment of  
the transaction based on the match results obtained  
in the authentication method.

35

09700305-000101

8. An authentication system for authenticating users who are parties to a transaction, the system comprising:

- (a) a unit supplying a first user with a matching key for a prospective transaction;
- (b) a unit receiving at a second user the matching key supplied to the first user; and
- (c) a unit matching a key supplied from the first user to the second user with the key supplied from the second user to the first user.

9. A user apparatus for authenticating a plurality of users who are parties to a transaction, the apparatus comprising:

- a first transmitting unit that transmits information concerning a prospective transaction to an authentication system that supplies different matching keys to the users;

- a first receiving unit that receives the matching keys to the transaction sent from the authentication system in response to transmitted information concerning the prospective transaction;

- a second transmitting unit that exchanges matching keys between the users, and transmits the exchanged matching keys to the authentication system for matching; and

- a second receiving unit that receives match results from the authentication system.

35

10. A computer-readable medium storing program code for causing a computer to authenticate

097883000, 00000000

users who are parties to a transaction, the program code comprising:

5 a first program code segment that causes a first transmitting unit to transmit information concerning a prospective transaction to an authentication system that supplies different matching keys to the users;

10 a second program code segment that causes a first receiving unit to receive the matching keys to the transaction from the authentication system in response to transmitted information concerning the prospective transaction;

15 a third program code segment that causes a second transmitting unit to exchange matching keys between the users, and transmits the exchanged matching keys to the authentication system for matching; and

20 a fourth program code segment that causes a second receiving unit to receive match results from the authentication system.

25 11. An apparatus comprising a computer-readable medium storing program code for causing a computer to verify users who are parties to a transaction, the program code comprising:

30 a first program code segment that causes a first transmitting unit to transmit information concerning a prospective transaction to an authentication system that supplies different matching keys to the users;

35 a second program code segment that causes a first receiving unit to receive the matching keys to the transaction from the authentication system in response to transmitted information concerning the

2025 RELEASE UNDER E.O. 14176